

Application Number 09/907,230

Responsive to Office Action mailed July 27, 2005

REMARKS

This Amendment is responsive to the Final Office Action dated July 27, 2005 and constitutes the required submission with a request for continued examination (RCE). Applicants have amended claims 1-6, 9, 15-19, 21, 23 and 29-32, and added new claim 38. Claims 1-38 are now pending.

As a preliminary matter, Applicants note that an Information Disclosure Statement (IDS) is being submitted in parallel with this response. Applicants respectfully request that the Examiner consider the reference listed in the IDS and return an initialed Form 1449 to Applicants.

In the Final Office Action, the Examiner rejected claims 1-6, 8-10, 12, 14-25, 27-32 and 34-37 under 35 U.S.C. 102(b) as being anticipated by Sollish (WO 98/08180). The Examiner also rejected claims 7 and 11 under 35 U.S.C. 103(a) as being unpatentable over Sollish in view of Stebbings (6,684,199); rejected claims 13 and 33 under 35 U.S.C. 103(a) as being unpatentable over Sollish in view of Bell (6,832,319); and rejected claim 26 under 35 U.S.C. 103(a) as being unpatentable over Sollish in view of Menezes (Handbook of Applied Cryptography, CRC Press, 1997, pg. 363).

In response to these rejections, Applicants have amended all pending claims to clarify the claimed invention for the Examiner. Applicants respectfully traverse the rejections to the extent such rejections may be considered applicable to the amended claims. The applied references fail to disclose or suggest the inventions defined by Applicants' claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

More specifically, Applicants have amended all pending claims to make two fundamental clarifications. First, the amended claims clarify that the invention concerns the prevention of the creation of unauthorized copies of a medium. In stark contrast, the passages of Sollish, which are relied upon by the Examiner in rejecting all pending claims, are actually the antithesis of this new requirement to Applicants' pending claims because the cited passages describe techniques for overriding error correction.

Applicants recognize that Sollish is generally concerned with thwarting unauthorized copying. To do this, Sollish makes use of what is referred to as "Ambiguous Symbols." According to Sollish, when an ordinary copy is made of optical media containing one or more

Application Number 09/907,230

Responsive to Office Action mailed July 27, 2005

Ambiguous Symbols, the copy will not contain such Ambiguous Symbols because standard optical equipment cannot write such Ambiguous Symbols. A media player designed to require Ambiguous Symbols, then, can associate the absence of such symbols with an unauthorized copy.

The passages of Sollish relied upon by the Examiner as disclosing uncorrected data and incorrect error correction information (as required by Applicants' claims), however, do not concern the prevention of unauthorized copying. Quite the contrary, the passages of Sollish relied upon by the Examiner describe techniques for overriding error correction, to thereby disable the copy protection techniques of Sollish that rely upon error correction to eliminate Ambiguous Symbols.

Thus, whereas Applicants' claims require the prevention of the creation of unauthorized copies of a medium, the relied upon passages of Sollish concern techniques for disabling copy protection, i.e., allowing unauthorized copying. In view of the amendment to the claims, Applicants believe that the teaching of Sollish relied upon by the Examiner has been clearly overcome in this respect.

Nevertheless, a second clarification to Applicants' claims has also been made to more clearly specify an "access key" and further clarify that the erroneous error correction information is included in the access key. In Sollish, incorrect error correction information is not contained within an access key.

In particular, all pending claims have been amended to clarify that the access key facilitates access to digital content on the medium and includes uncorrected data and associated error correction information, wherein the error correction information of the access key includes one or more errors. Nothing in Sollish discloses or suggests an access key that facilitates access to digital content on the medium, wherein the access key includes erroneous error correction information.

In the Office Action, the Examiner interpreted the passage of Sollish on page 17, lines 22-24, as teaching an access key that includes uncorrected data and associated erroneous error correction information. However, contrary to the Examiner's interpretation of Sollish, nothing in Sollish suggests an access key that includes erroneous error correction information. To the extent that Sollish discloses data having uncorrected data and associated erroneous error

Application Number 09/907,230

Responsive to Office Action mailed July 27, 2005

correction information, this data is not an access key that facilitates access to digital content. Instead, in Sollish, erroneous symbols are introduced into the ECC portion of a codeword, i.e., into the content, and not into a key that is used to access the content.

Furthermore, as noted above, in Sollish the erroneous symbols are introduced into the ECC portion of a codeword in order to allow copying, rather than to prevent creation of unauthorized copies.

None of the secondary references applied by the Examiner (including Bell, Stebbings, or Menezes) provides any teaching that would remedy the fundamental differences of Sollish relative to Applicants' pending independent claims. Therefore, all pending claims should be in condition for allowance.

New claim 38 has been added to further require that the access key comprises a cryptographic access key that facilitates decryption of the digital content on the medium. Neither Sollish nor any of the other applied references discloses or suggests a cryptographic access key that facilitates decryption of the digital content on the medium, wherein the cryptographic access key includes erroneous error correction information.

Applicants have also amended many claims for reasons unrelated to patentability, i.e., to improve clarity.

Dependent claim 5 has also been further amended to recite that controlling access to the digital content on the medium includes copying the digital content from the medium to a second medium, applying the error correction information to the uncorrected data to produce a second access key, and copying the second access key to the second medium. In addition, dependent claim 5 requires that the second access key is corrupted by the one or more errors such that the second access key does not facilitate access to the copied digital content on the second medium. Applicants believe that the amendments to dependent claim 5 even further distinguish all of the applied prior art.

With regard to the rejection of claim 13, Applicants are confused by the Examiner's reliance on Bell. The Examiner rejected claim 13 under 35 U.S.C. 103(a) as being unpatentable over Sollish in view of Bell.

Claim 13 is dependent upon claim 1, and clarifies that selecting the access key includes assigning a random number to the medium, wherein the random number is uniquely associated

Application Number 09/907,230

Responsive to Office Action mailed July 27, 2005

with the medium, selecting the access key from the plurality of access keys based on the random number, generating a hash value from the random number and the selected access key, and decrypting content of the medium using the hash value.

In rejecting claim 13, the Examiner indicated that column 2, lines 44-47, of Bell discloses assigning a random number to the medium, wherein the random number is uniquely associated with the medium. While this passage of Bell does describe the use of media ID, nothing in this passage suggests that media ID is a random number assigned to the medium.

Furthermore, in rejecting claim 13, the Examiner relied upon column 4, lines 40-54, of Bell as teaching the selection of the access key from the plurality of access keys based on the random number, the generation of a hash value from the random number and the selected access key, and the decrypting of content of the medium using the hash value. Unfortunately, this passage of Bell lacks any teaching of these features claim 13.

The passage of Bell at column 4, lines 40-54 is copied below in its entirety:

In another aspect, a user computer program storage device is accessible by a player-recorder establishing a player and a recorder. As disclosed in detail below, the user computer program storage device includes computer readable code means for sending encrypted data from a data storage medium to the player. Computer readable code means read a media identification and a media key block on the data storage medium, and computer readable code means then determine a media key using the media key block. Additionally, computer readable code means determine a content key using the media key and the media identification, such that computer readable code means can decrypt data on the data storage medium using the content key to facilitate the player playing video and/or audio represented by the data.

Nothing in this passage of Bell suggests the selection of the access key from a plurality of access keys based on the random number, nor the generation of a hash value from the random number and the selected access key, nor the decrypting of content of the medium using the hash value. Thus, it appears that every limitation of claim 13 is lacking from the cited passage of Bell.

More specifically, nothing in this passage of Bell discusses a "plurality of access keys" whatsoever, much less the selection of the access key from a plurality of access keys based on the random number. In addition, nothing in this passage discusses a "hash value" whatsoever, much less generating a hash value from the random number and decrypting of content of the medium using the hash value. In view of these clear deficiencies, Applicants request a favorable indication of patentability with respect to dependent claim 13.

Application Number 09/907,230

Responsive to Office Action mailed July 27, 2005

CONCLUSION

For at least the reasons set forth above, all claims in this application are in condition for allowance. Applicants respectfully request reconsideration and prompt allowance of all pending claims. With regard to any claims or features not specifically addressed herein, Applicants do not acquiesce to any of the rejections or characterizations of the prior art, and reserve the right to further address other the features of the independent claims or dependent claims, if necessary.

Please charge any additional fees or credit any overpayment to Deposit Account No. 09-0069. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date:

10/18/05

Imation Legal Affairs
P.O. Box 64898
St. Paul, Minnesota 55164-0898
Telephone: (651) 704-3604
Facsimile: (651) 704-5951

By:



Name: Eric D. Levinson
Reg. No.: 35,814